IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

		Attorney Docket No.: **CA920030040US1**
In re Application of:	§	
	§	Confirmation No.: **7948**
YANTZI	§	
	§	Examiner: **POLTORAK, P.**
Serial No.: **10/809,563**	§	
	§	Art Unit: **2134**
Filed: **25 MARCH 2004**	§	
	§	
For: **PASSWORD MANAGEMENT**	§	

APPEAL BRIEF

MS Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The present Appeal Brief is submitted in support of the Appeal in the above-identified application.

Please charge IBM Deposit Account No. **09-0447** in the amount of $540.00 for the submission of the present Brief. No additional fee or extension of time is believed to be required; however, in the event an additional fee or extension of time is required, please charge that fee to IBM Deposit Account No. **09-0447**.

TABLE OF CONTENTS

REAL PARTY IN INTEREST

The present application is assigned to International Business Machines Corporation, the real party of interest.

RELATED APPEALS AND INTERFERENCES

No related appeal is presently pending.

STATUS OF THE CLAIMS

Claims 1 and 26, which were finally rejected by the Examiner as noted in the Final Office Action dated August 15, 2008, are being appealed.

STATUS OF AMENDMENTS

An Amendment was submitted on November 13, 2007 in reply to the Non-Final Office Action dated September 12, 2007. An Amendment was submitted on February 18, 2008 in reply to the Final Office Action dated December 18, 2007. An Amendment was submitted on June 10, 2008 in reply to the non-Final Office Action dated May 21, 2008.

SUMMARY OF THE CLAIMED SUBJECT MATTER

Claim 1 recites a method of managing passwords for a set of software resources accessible by a user. A password registry is provided for storing passwords within a workstation (page 6, lines 6-7; password registry **210** of Figure **2**). Each of the software resources is allowed to register its password in the password registry via a respective one of the front-end processes within the workstation (page 7, lines 1-3; Figure **2**). Each of the passwords is encrypted by the respective front-end process before being stored in the password registry (page 8, lines 6-8; Figure **2**). In response to an access request to one of the software resources via a corresponding one of the front-end processes, a determination is made whether or not an encrypted password associated with the requested software resource is stored in the password registry (page 9, lines 17-20; block **3** of Figure **3B**). If the encrypted password associated within the requested software resource is stored in the password registry, the encrypted password is sent from the password registry to the corresponding front-end process for decryption in order to permit the access request (page 10, lines 1-2; block **4** of Figure **3B**). If the encrypted password associated within the requested software resource is not stored in the password registry, the front-end process is notified to prompt for a password from a user (page 10, line 24 - page 11, line 3; block **6** of Figure **3C**).

Claim 26 recites a computer readable medium having computer program product for managing passwords for a set of software resources accessible by a user. The computer readable medium includes computer program code for providing a password registry to store passwords within a workstation (page 6, lines 6-7; password registry **210** of Figure **2**). Each of the software resources is allowed to register its password in the password registry via a respective one of the front-end processes within the workstation (page 7, lines 1-3; Figure **2**). Each of the passwords is encrypted by the respective front-end process before being stored in the password registry (page 8, lines 6-8; Figure **2**). The computer readable medium also includes computer program code for, in response to an access request to one of the software resources via a corresponding one of the front-end processes, determining whether or not an encrypted password associated with the requested software resource is stored in the password registry (page 9, lines 17-20; block **3** of Figure **3B**). If the encrypted password associated within the requested software resource is stored in the password registry, the encrypted password is sent from the password registry to the corresponding front-end process for decryption in order to permit the access request (page 10, lines 1-2; block **4** of Figure **3B**). If the encrypted password associated within the requested software resource is not stored in the password registry, the front-end process is notified to prompt for a password from a user (page 10, line 24 - page 11, line 3; block **6** of Figure **3C**).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The Examiner's rejection of Claims 1 and 26 under 35 U.S.C. § 102(b) as being anticipated by *Nielsen* (US 6,182,229).

ARGUMENT

The Examiner's rejection of Claims 1 and 26 is not well-founded and should be reversed.

I. *Nielson* does not disclose the claimed password registry and registration process

Claim 1 (and similarly Claim 26) recites a step of "providing a password registry for storing passwords within a workstation" and a step of "allowing each of a plurality of software resources to register its password in said password registry via a respective one of a plurality of front-end processes within said workstation..."

On page 4 of the Final Office Action, the Examiner asserts that the claimed password registry is disclosed by *Nielsen* in the Abstract section as "database of encrypted password." According to *Nielsen*, a user at "a client system may access a plurality of remote servers requiring passwords for access ... [and] the client system maintains a database of encrypted passwords and user IDs for remote servers to which the user is registered." Thus, the "database of encrypted password" is located within *Nielsen*'s client system (and not *Nielsen*'s remote systems). In contrast, the claimed password registry is located at a workstation that is more similar to *Nielsen*'s remote servers instead of *Nielsen*'s client system, such interpretation is based on the perspective of Claim 1 as well as Figure **1** of the specification. As such, *Nielsen* does not disclose the claimed providing step.

On page 4 of the Final Office Action, the Examiner asserts that the claimed allowing step is disclosed by *Nielsen* in Figure **1B** and in col. 1, lines 32-43. However, neither Figure **1B** nor col. 1, lines 32-43 of *Nielsen* teaches the claimed multiple front-end processes within a workstation.

On page 2 of the Final Office Action, the Examiner attempts to characterize all processes within the *Nielsen*'s workstation as the claimed front-end processes. Assuming *arguendo* that the Examiner's characterization can be considered as acceptable, *Nielsen* still has not disclosed the claimed password registration process because *Nielsen* does not disclose the registration of passwords at the "database of encrypted password" that the Examiner has previously characterized as the claimed password registry. As such, *Nielsen* does not disclose the allowance of each of multiple software resources "to register its password in said password registry via a respective one of a plurality of front-end processes within said workstation," as claimed.

II. *Nielson* does not disclose the claimed determining and sending steps

Claim 1 also recites a step of "in response to an access request to one of said software resources via a corresponding one of said front-end processes, determining if an encrypted password associated with said requested software resource is stored in said password registry" and a step of "in a determination that said encrypted password associated within said requested software resource is stored in said password registry, sending said encrypted password from said password registry to said corresponding front-end process for decryption in order to permit said access request."

On pages 3 and 5 of the Final Office Action, the Examiner asserts that the claimed determining step and the claimed sending step are disclosed by *Nielsen* in col. 4, lines 46-64. According to *Nielsen* in col. 4, line 60-64, "the database of FIG. **2** is scanned for an entry having the URL of the website sending the authentication request. If an entry is found, the password management system decrypts the password and user ID information using the master password as a key at step **314**." The database of Figure **2** is located within *Nielsen*'s client system (as mentioned above), and scanning of the database of Figure **2** is preformed <u>in response to a user attempting to access a control access web site</u> that sends an authentication request to client computer system **10**, and the password management system intercepts the request by inhibiting its display and attempts to respond to the authentication request automatically (col. 4, lines 48-59). In contrast, the claimed determining step is performed "in response to an access request to one of said software resources via a corresponding one of said front-end processes."

According to *Nielson*, after the password management system has decrypted the password and user ID information using the master password as a key, the password and user ID information are sent to the remote site (col. 5, lines 1-4). In contrast, the claimed sending step sends the encrypted password "from said password registry to said corresponding front-end process for decryption in order to permit said access request."

III. *Nielsen* does not disclose the claimed notifiying step

In addition, Claim 1 recites a step of "in a determination that said encrypted password associated within said requested software resource is not stored in said password registry, notifying said front-end process to prompt for a password from a user."

On page 5 of the Final Office Action, the Examiner asserts that the claimed notifying step is disclosed by *Nielsen* in col. 4, lines 64-66. To continued with the above-mentioned process of *Nielsen*, if an entry is found in the database of Figure **2**, the password management system decryptes the password and user ID information using the master password as a key, but if the master password was not entered by a user at step **302** due to the preference setting, the user is prompted for it now (col. 4, lines 60-66). Instead of a master password not entered by a user, the claimed invention recites "in a determination that said encrypted password associated within said requested software resource is not stored in said password registry."

Because of the claimed invention includes novel features that are not disclosed by *Nielson*, the § 102 rejection is improper.

CONCLUSION

For the reasons stated above, Appellants believe that the claimed invention to be patentably distinct over the cited references, and that the rejections under 35 U.S.C. § 102 are not well-founded. Hence, Appellants respectfully urge the Board to reverse the Examiner's rejection.

Respectfully submitted,

Antony P. Ng
Registration No. 43,427
DILLON & YUDELL, LLP
8911 N. Cap. of Texas Hwy., suite 2110
Austin, Texas 78759
(512) 343-6116

ATTORNEY FOR APPELLANTS

CLAIMS APPENDIX

1. A method of managing passwords for a plurality of software resources accessible by a user, said method comprising:

providing a password registry for storing passwords within a workstation;

allowing each of a plurality of software resources to register its password in said password registry via a respective one of a plurality of front-end processes within said workstation, wherein each said password is encrypted by said respective front-end process before being stored in said password registry;

in response to an access request to one of said software resources via a corresponding one of said front-end processes, determining if an encrypted password associated with said requested software resource is stored in said password registry;

in a determination that said encrypted password associated within said requested software resource is stored in said password registry, sending said encrypted password from said password registry to said corresponding front-end process for decryption in order to permit said access request; and

in a determination that said encrypted password associated within said requested software resource is not stored in said password registry, notifying said front-end process to prompt for a password from a user.

2. The method of claim 1, wherein said method further includes associating each of said encrypted passwords with an identifying information.

3. The method of claim 2, wherein said identifying information includes at least one of a user ID, a resource hostname, and a resource type.

4. The method of claim 3, wherein said method further includes utilizing at least one of said user ID, said resource hostname, and said resource type as a query key to uniquely identify said each software resource and its associated encrypted password.

5. The method of claim 4, wherein said method further includes retrieving a corresponding one of said encrypted passwords using said query key.

6-25. canceled

26. A computer readable medium having computer program product for managing passwords for a plurality of software resources accessible by a user, said computer readable medium comprising:

computer program code for providing a password registry for storing passwords within a workstation;

computer program code for allowing each of a plurality of software resources to register its password in said password registry via a respective one of a plurality of front-end processes within said workstation, wherein each said password is encrypted by said respective front-end process before being stored in said password registry;

computer program code for, in response to an access request to one of said software resources via a corresponding one of said front-end processes, determining if an encrypted password associated with said requested software resource is stored in said password registry;

computer program code for, in a determination that said encrypted password associated within said requested software resource is stored in said password registry, sending said encrypted password from said password registry to said corresponding front-end process for decryption in order to permit said access request; and computer program code for, in a determination that said encrypted password associated within said requested software resource is not stored in said password registry, notifying said front-end process to prompt for a password from a user.

27. The computer readable medium of claim 26, wherein said computer readable medium further includes computer program code for associating each said encrypted password with an identifying information.

28. The computer readable medium of claim 27, wherein said identifying information includes at least one of a user ID, a resource hostname, and a resource type.

29. The computer readable medium of claim 28, wherein said computer readable medium further includes computer program code for utilizing at least one of said user ID, said resource hostname, and said resource type as a query key to uniquely identify said each software resource and its associated encrypted password.

30. The computer readable medium of claim 29, wherein said computer readable medium further includes computer program code for retrieving a corresponding one of said encrypted passwords using said query key.

EVIDENCE APPENDIX

Other than the Office Actions and Responses already of record, no additional evidence has been entered by Appellants that is relevant to the present appeal.

RELATED PROCEEDINGS APPENDIX

There is no related proceeding as described by 37 C.F.R. § 41.37(c)(1)(x) known to Appellants, Appellants' legal representative or assignee.